Surjectivity in Honda-Tate

Brian Lawrence

May 5, 2014

1 Introduction

Let $\mathbb{F}_q$ be a finite field with $q = p^a$ elements, p prime. Given any simple Abelian variety A over $\mathbb{F}_q$, we have seen that the characteristic polynomial π_A of Frobenius acting on A is a polynomial with integer coefficients whose roots are Weil q-integers. So we have a map

$$HT_q : \{\text{simple abelian varieties over } F_q, \text{ up to isogeny}\} \to \{\text{Weil } q\text{-integers, up to conjugacy}\}.$$

We have seen that this map is well-defined and injective; we still have to show that it is surjective.

In concrete terms, given a Weil q-integer π, we need to construct a simple abelian variety over $\mathbb{F}_q$ on which the Frobenius element acts as π. The only known construction is by reducing a CM abelian variety from characteristic zero. Specifically, our construction will proceed in five steps.

First, fix a CM field L containing $\mathbb{Q}[\pi]$, and a CM type (L, Φ). (The field L and data Φ will be determined later.) Construct an abelian variety A_0 over $\mathbb{C}$ of this CM type. In particular, A_0 has an action by the element $\pi \in L$, and this automorphism has the desired characteristic polynomial.

Second, show that A_0 is in fact defined over a number field K.

Third, show that A_0 has good reduction at a place v of K over p. Thus the identity component of the special fiber is an abelian variety A, defined over some field of characteristic p, whose endomorphism ring contains L.

Fourth, determine the Frobenius action on A. More precisely, we will see that the Frobenius element of A comes from an element π_A of L, and determine its valuation at every place of L. By a judicious choice of (L, Φ) we can arrange that π_A is "almost" π, in a sense which will be made precise.

Fifth, argue that π itself must be in the image of the map HT_q.

2 Complex Multiplication over $\mathbb{C}$

We want to make an abelian variety over $\mathbb{C}$ with an action by the Weil q-integer π, in the hopes that later this action will turn into a Frobenius action in characteristic p. The idea is to make a CM abelian variety with this action.

First, we review the basic theory of abelian varieties over $\mathbb{C}$, and in particular the theory of complex multiplication. Mumford's book [Mu1] is a good reference for the material in this section.

Any proper group variety A over $\mathbb{C}$ must be abelian, so the exponential map from the Lie algebra $\mathrm{Lie}\, A \to A$ is a group homomorphism, with $\mathrm{Lie}\, A$ regarded as an abelian group. If g is the dimension of A then we obtain an isomorphism

$$V/\Lambda \equiv A,$$

where Λ is a lattice of rank $2g$ in a g-dimensional $\mathbb{C}$-vector space V (namely, $V = \mathrm{Lie}\, A$.

Conversely, given any such (V, Λ), the quotient V/Λ is a compact analytic manifold which may or may not be algebraic. In fact it is algebraic if and only if the lattice Λ satisfies the Riemann bilinear relations. See the Corollary to the Theorem of Lefschetz at the end of Section 3 of [Mu1] for a precise statement and proof. (In dimension 1, every analytic torus is algebraic; this is one way in which the general theory of abelian varieties differs from the special case of elliptic curves.)

Now suppose we are given an (algebraic) abelian variety A, with an expression as a quotient V/Λ. Then any holomorphic automorphism of A lifts to a linear automorphism of the universal covering space V; conversely, a linear automorphism of V arises from a holomorphic map $A \to A$ if and only if it carries the lattice Λ into itself.

Definition 2.1. *We say an abelian variety is* simple *if it is not isogenous to the direct product of two abelian varieties of lower dimension.*

By Poincare's Complete Reducibility Theorem, every abelian variety is isogenous to a product of simple varieties.

Theorem 2.2. *If an order in a field L is contained in the endomorphism ring of an abelian variety A of dimension g over $\mathbb{C}$, then $[L : \mathbb{Q}]$ divides $2g$.*

Proof. The action of L on $A = V/\Lambda$ lifts to a linear action on V preserving the lattice Λ. Thus, L acts on $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$, making the rational vector space $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ into an L-vector space. □

This motivates the following definition.

Definition 2.3. *We say that an abelian variety A of dimension g has* complex multiplication *(or is a* CM abelian variety*, or is of* CM type*) if its endomorphism algebra (i. e.* $\mathrm{End}\, A \otimes \mathbb{Q}$*) contains a semisimple commutative subalgebra L of degree $2g$. In this case we also say that A has* complex multiplication by L*, or by the order in L consisting of elements which map to bona fide endomorphisms of A.*

Remark 2.4. *If a simple abelian variety has complex multiplication then in fact the commutative algebra mentioned above must be a field.*

If, in addition, the base field has characteristic zero, then one can show that the field L must be a CM field. By further use of Poincaré reducibility it is a good exercise to check that if A is an abelian variety over $\mathbb{C}$ with CM then its isotypic parts have CM and moreover admit CM by a CM field. In other words, the abelian varieties over $\mathbb{C}$ which admit CM by a CM field are precisely the isotypic CM abelian varieties.

Suppose we are given some

$$A \equiv V/\Lambda$$

which admits complex multiplication by a CM field L. Since the rational homology $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ is thereby 1-dimensional over L, the Hodge decomposition of the complexified homology makes the $L \otimes_{\mathbb{Q}} \mathbb{C}$-linear quotient $\mathrm{Lie}(A)$ an invertible module over $\mathbb{C}_\Phi = \prod_{\varphi \in \Phi} \mathbb{C}$ for some collection Φ of g embeddings of L which contains one from each conjugate pair of embeddings. (The L-linear structure is encoded by $\ell.(x_\varphi) = (\varphi(\ell)x_\varphi)$). By choosing a basis of Λ as a 1-dimensional L-vector space, we thereby identify $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{Lie}(A)$ with the natural inclusion of L into $\mathbb{C}_\Phi$, and in this way Λ is commensurable with the ring of integers of L inside L. Hence, A is L-linearly isogenous to $\mathbb{C}_\Phi/\mathcal{O}_L$. Thus, the L-linear isogeny class of the abelian variety A is determined by the field L and the choice of Φ. Such a pair (L, Φ) is called a *CM type*.

We have seen that every isotypic CM abelian variety over $\mathbb{C}$ determines a CM type (L, Φ). Conversely, given a CM type, we can ask whether the quotient $\mathbb{C}_\Phi/\mathcal{O}_L$ is algebraizable (in which case the same holds for all lattices in $L \subset \mathbb{C}_\Phi$. It is an elementary calculation in algebraic number theory to verify that the Riemann bilinear relations are always satisfied for a lattice arising in this way, so the torus is indeed algebraizable. One can also characterize in terms of (L, Φ) when this construction is *simple* as an abelian variety, but we omit that. Summarizing, we have the following theorem.

Theorem 2.5. *Given any CM field L of degree $2g$, and CM type (L, Φ), there is an abelian variety A of dimension g over $\mathbb{C}$, of the given CM type. Furthermore, this A is unique up to L-linear isogeny.*

Remark 2.6. *It is possible to define CM types for isotypic CM abelian varieties over any algebraically closed field k of characteristic zero. Instead of working with the analytic uniformization, we consider the k-linear action of the CM field L on the tangent space to A at the origin. As before, we obtain a set Φ of g embeddings of L in k. Since L must be a CM field, it has an intrinsically defined complex conjugation, so it still makes sense (and it turns out to be correct) that Φ contains one embedding from each conjugate pair. We will make use of CM types over local fields below.*

At this point we need an easy lemma.

Lemma 2.7. *If π is a Weil q-number then $\mathbb{Q}[\pi]$ is either a CM field or a totally real field.*

Proof. Suppose first that π is not real. Since for every conjugate ρ of π we have $|\rho| = \sqrt{q}$, we see that $\rho + q/\rho$ is real. Thus, $\mathbb{Q}[\pi + q/\pi]$ is a totally real field, over which $\mathbb{Q}[\pi]$ has degree two. Hence, $\mathbb{Q}[\pi]$ is CM.

If on the other hand π is real, then we must have $\pi = \pm\sqrt{q}$, and the result follows. □

The first step of our construction is as follows. Given our Weil q-number π, fix some CM field L containing π, and some CM type (L, Φ), to be chosen later. (The lemma above guarantees the existence of the field L.) Let A_0 be the abelian variety defined over $\mathbb{C}$ of this CM type.

3 Descent to a Number Field

We wish to show that every abelian variety with complex multiplication over $\mathbb{C}$ is in fact defined over a number field. We may and do focus on the isotypic case, so there is a CM structure by a CM field. There are two approaches to this result, one using moduli of abelian varieties, and one using specialization. We will outline the proof using moduli and give a thorough proof using the specialization method.

For the first approach, one constructs a moduli space of principally polarized abelian varieties with sufficient level structure and complex multiplication by a given order in a given CM field, and show that this has only countably many points over $\mathbb{C}$ and hence has dimension zero. It follows that every $\mathbb{C}$-point of the moduli space in fact comes from a $\overline{\mathbb{Q}}$-point, and hence that our abelian variety A_0, along with its complex multiplication, descend to a finite extension of $\mathbb{Q}$. The construction of the moduli space relies on deep results with Hilbert schemes which we do not wish to discuss.

For the remainder of this section fix an embedding $\overline{\mathbb{Q}} \to \mathbb{C}$. The key result is the following "specialization" lemma.

Lemma 3.1. *Let L be a CM field, $\mathcal{O}$ an order in L, and suppose A is an abelian variety over $\mathbb{C}$ with a CM action of $\mathcal{O}$, of CM type (L, Φ). Then there is an abelian variety A_0 defined over $\overline{\mathbb{Q}}$, also having CM by $\mathcal{O}$ of CM type (L, Φ).*

Proof. Observe that $\mathbb{C}$ is trivially a direct limit of its finitely-generated $\overline{\mathbb{Q}}$-subalgebras. Thus, by standard results, the abelian variety A together with the action of $\mathcal{O}$ descends to an abelian scheme with $\mathcal{O}$-action over a finitely-generated $\overline{\mathbb{Q}}$-algebra R.

By localizing R, we may assume that the tangent space Lie A, a priori locally free over R, is in fact free. Now since R contains $\overline{\mathbb{Q}}$, and in particular the Galois closure of L in $\overline{\mathbb{Q}}$, we see by further localization around the generic point of $\mathrm{Spec}(R)$ that the action of $\mathcal{O}$ on Lie A decomposes as a sum of free modules of rank 1 on which the actions are given by the CM type Φ.

Let m be a maximal ideal of R. Then by Hilbert's Nullstellensatz, R/m is isomorphic to $\overline{\mathbb{Q}}$. The fiber of A at m is then an abelian variety over $R/m \equiv \overline{\mathbb{Q}}$, with complex multiplication by $\mathcal{O}$ and of CM type (L, Φ). □

Remark 3.2. *In the notation of Lemma 3.1, one can in fact show that the original abelian variety A is defined over $\overline{\mathbb{Q}}$ as well. This is because A must be isogenous to A_0, and any isogeny from A_0 must be defined over $\overline{\mathbb{Q}}$. We will not use this fact, so we do not give a detailed proof.*

Now we have constructed an abelian variety A_0 of CM type (L, Φ), defined over $\overline{\mathbb{Q}}$. Again by standard arguments, A_0 and the CM action are in fact defined over a number field K.

4 Reduction to a Finite Field

Now we have an abelian variety A_0, with complex multiplication by an order in the CM field L, defined over a number field K, and we wish to show obtain from this an abelian variety over a finite field of characteristic p. To do this we need to know something about the reduction of A_0 at a place of K lying over p. In general, the semi-abelian reduction theorem guarantees that the connected component of the special fiber of the Néron model is an extension of an abelian variety by a torus; we will see that in the case of a reduction of a CM curve, the torus must be trivial.

We have the following result on reduction of abelian varieties. See [BLR], Section 7.4, Theorem 1.

Lemma 4.1. *Let A_0 be an abelian variety defined over a number field K. Then there is a finite Galois extension K' of K such that the Néron model $\mathcal{A}_0$ of A_0 over the ring of integers $\mathcal{O}_{K'}$ of K' has semi-abelian reduction at every place of K'. This means that the identity component of the fiber of $\mathcal{A}_0$ over every closed point of* $\operatorname{Spec} \mathcal{O}_{K'}$ *is an extension of an abelian variety by an affine torus.*

In the case of a CM abelian variety, the special fiber must in fact be abelian, not just semi-abelian; and in fact the special fiber must itself have an action of the CM field. This is the content of the following theorem.

Theorem 4.2. *Let A_0 be a CM abelian variety, with complex multiplication by an order $\mathcal{O}$ in a number field L, defined over a number field K. With notation as in the previous lemma, the identity component of the fiber of $\mathcal{A}_0$ over every closed point of* $\operatorname{Spec} \mathcal{O}_{K'}$ *is an abelian variety, on which $\mathcal{O}$ acts via endomorphisms.*

Proof. Let A denote the identity component of the fiber of $\mathcal{A}_0$ over some closed point of $\operatorname{Spec} \mathcal{O}_{K'}$.

By the Néron mapping property (see Section 1.2 of [BLR]), every automorphism of the abelian variety A_0 extends uniquely to an automorphism of the Néron model $\mathcal{A}_0$ over $\operatorname{Spec} \mathcal{O}_{K'}$, and this in turn restricts to an automorphism of the fiber. Thus in particular the order $\mathcal{O}$ in the CM field L acts via endomorphisms on fiber. Since any endomorphism must take the identity component to itself, $\mathcal{O}$ also acts via endomorphisms on A. This gives the second part of the theorem.

We now use the CM action to prove the first part, as follows. By the lemma on semi-abelian reduction (Lemma 4.1) we know that A fits in a short exact sequence (of group varieties over the residue field of $\operatorname{Spec} \mathcal{O}_{K'}$)

$$0 \to T \to A \to B \to 0,$$

with T a torus and B an abelian variety. We must prove that T is trivial.

Since the factorization of A above is canonical, $\mathcal{O}$ acts via endomorphisms on T. Since an endomorphism of a torus induces a ($\mathbb{Z}$-linear) automorphism of its character lattice, we see that $\mathcal{O}$ acts on the character lattice $\chi(T)$, making it into an $\mathcal{O}$-module.

Thus, $\chi(T) \otimes \mathbb{Q}$ has the structure of an L-vector space. On the other hand, if d is the dimension of T, then $\chi(T)$ is a free lattice of rank d, so that $2g$ divides d. Since clearly $d \leq g$, we have $d = 0$, so T is trivial and $A \equiv B$ is an abelian variety, as desired. □

Applying the theorem at a place of $\operatorname{Spec} \mathcal{O}_{K'}$ over the prime factor p of q, we obtain an abelian variety A over a finite field F_{q_A} of characteristic p, with an action of $\mathcal{O}$ on A.

5 Computation of Frobenius

We now have an abelian variety A with an action by a CM field containing the given Weil q-integer π. But at present we have no information on the Frobenius action on A. We now seek to remedy this situation. In particular, we hope that by a judicious choice of the data (L, Φ), we can arrange that the Frobenius element π_A in the endomorphism algebra of A approximates π. Specifically, we will use L and Φ to get control over the valuation of π_A at every place of L, and hence guarantee that some power of π_A is equal to some power of π.

Lemma 5.1. *The relative Frobenius automorphism π_A of A lies in L, which is viewed as a subfield of $\operatorname{End}^0 A$ via the map $L \to \operatorname{End}^0 A$.*

Proof. Since all endomorphisms of A as an $\mathbb{F}_{q_A}$-variety must commute with π_A, we see that F and π_A must generate a commutative subfield of the endomorphism algebra $\operatorname{End}^0 A$. But by the Corollary at the end of Section 19 of [Mu1], this subfield can have degree at most $2g$ over $\mathbb{Q}$. Since $[L : \mathbb{Q}] = 2g$, so that π_A must lie in L. □

Rather than determine π_A directly as an element of L, we will calculate its valuation at every place of L. We adopt the "logarithmic" convention for nonarchimedean valuations: for such a valuation v we have $v(1) = 0$ and $v(ab) = v(a) + v(b)$.

Lemma 5.2. *The element π_A of L is a Weil q_A-integer. In particular, its absolute value with respect to every archimedian valuation is $\sqrt{q_A}$, and its valuation with respect to any nonarchimedean valuation is* 0.

Proof. The statement that π_A is a Weil q_A-integer is the Riemann hypothesis; it is roughly Theorem 4 of Section 21 of [Mu1]. (More precisely, [Mu1] shows in the discussion leading up to Theorem 4 that the characteristic polynomial of Frobenius on an abelian variety over $\mathbb{F}_{q_A}$ is a polynomial with integer coefficients, all of whose roots in $\mathbb{C}$ have absolute value $\sqrt{q_A}$. But it is clear that π_A, viewed as an endomorphism of A, satisfies its own characteristic polynomial; so as an element of L, it must be a Weil q_A-integer.)

The statement about the archimedean valuations follows immediately from the definition of a Weil q_A-integer.

Suppose v is a nonarchimedean valuation not lying over p. Since π_A is an algebraic *integer*, we have on one hand $v(\pi_A) \geq 0$. On the other hand, since its complex conjugate is also an algebraic integer, we have

$$v(\pi_A) \leq v(\pi_A) + v(\overline{\pi_A}) = v(q_A) = 0.$$

It follows from these two inequalities that $v(\pi_A) = 0$. □

That was easy! More difficult is to determine the valuation of the Frobenius element π_A at places lying over p. The answer will be given by the Shimura-Taniyama formula, below, after we establish some notation. The statement is taken from Paragraph 2.1.4.1 of [CCO]; see also Lemma 7.7 and surrounding text of [Eis].

Fix an algebraic closure $\overline{\mathbb{Q}}_p$. The number field L admits $[L : \mathbb{Q}] = 2g$ embeddings into $\overline{\mathbb{Q}}_p$. For each such embedding, the valuation on $\overline{\mathbb{Q}}_p$ pulls back to a valuation v on L that divides p. Conversely, given any such v, there are exactly $[L_v : \mathbb{Q}_p]$ embeddings of L into $\overline{\mathbb{Q}}_p$ such that the valuation on $\overline{\mathbb{Q}}_p$ pulls back to v. Denote by H_v the set of embeddings of L in $\overline{\mathbb{Q}}_p$ inducing the valuation v on L. The sets H_v, as v ranges over all places of L dividing p, partition the set H consisting of the $2g$ embeddings of L in $\overline{\mathbb{Q}}_p$.

Recall that our CM abelian variety A_0 was constructed from the number field L and a CM type Φ, which we regarded as a choice of g embeddings (satisfying some condition) of L into the base field $\mathbb{C}$. We have seen that A_0 can be defined over a number field; and certainly by tensoring to a completion we can regard it as being defined over $\overline{\mathbb{Q}}_p$. But now by Remark 2.6, we may regard Φ as a set of g embeddings of L into $\overline{\mathbb{Q}}_p$, one from each conjugate pair. (Again, we recall that the complex conjugation on the CM field L is intrinsically defined.)

We can now state the Shimura-Taniyama formula.

Theorem 5.3. *Let (L, Φ), A_0, A, q_A, and π_A be as above. Then for each place v of L dividing p, we have*

$$\frac{v(\pi_A)}{q_A} = \frac{\#(\Phi \cap H_v)}{\#H_v}.$$

The proof uses the theory of Dieudonné modules and p-divisible groups in mixed characteristic. The difficulty is in relating the CM type Φ, which only makes sense in characteristic zero, to the Frobenius element π_A, which arises

in characteristic p. These two are related by the p-power torsion of the group *scheme* over $\mathbb{Z}_\iota$; this torsion forms a p-divisible group which keeps track of the CM type Φ in characteristic zero and the Frobenius action in characteristic p. If time permits we will discuss Dieudonné modules and p-divisible groups next week, but only in characteristic p, not in mixed characteristic.

The Shimura-Taniyama formula, together with the easy lemma above, determines the valuation of π_A at every place of L. We now choose our CM type (L, Φ) so that π_A approximates π.

Theorem 5.4. *Given a Weil q-integer π, we can choose a number field L and a CM datum Φ such that, if A is the abelian variety over the finite field $\mathbb{F}_{q_A}$ constructed above, and $\pi_A \in L$ induces the Frobenius action on A, then for every place v of L dividing p, we have*

$$\frac{v(\pi_A)}{v(q_A)} = \frac{v(\pi)}{v(q)}.$$

Proof. By the Shimura-Taniyama formula, it is enough to choose L and Φ such that

$$\frac{\#(\Phi \cap H_v)}{\#H_v} = \frac{v(\pi)}{v(q)}$$

for every place v of L.

Suppose first that L is fixed, so that we need to determine whether there is a $\Phi \subset H$ satisfying the above equality, and containing one embedding from each conjugate pair. If the rational numbers

$$n_v := (\#H_v)\frac{v(\pi)}{v(q)}$$

are integers between 0 and $\#H_v$, inclusive, then we can choose a subset Φ of H such that the intersections $\Phi \cap H_v$ have the correct size. But we must in addition guarantee that Φ contains one embedding from each conjugate pair.

We discuss the conjugate pairs first. Let $\rho : L \to L$ be the complex conjugation, which we recall is intrinsic to L. Then ρ acts on the places of L over p via $(\rho v)(x) = v(\rho(x))$. In particular, precomposition with ρ gives a bijection between the sets H_v and $H_{\rho v}$. Thus, since $\pi\rho(\pi) = q$, we have

$$n_v + n_{\rho v} = (\#H_v)\left(\frac{v(\pi)}{v(q)} + \frac{v(\rho(\pi))}{v(\rho(q))}\right) = \#H_v = \#H_{\rho v}.$$

It now follows by an easy argument that, if the n_v are all integers satisfying $0 \le n_v \le \#H_v$, then we can find a subset $\Phi \in H$, containing one element from each conjugate pair, whose intersection with each H_v has exactly n_v elements.

It is also easy to see that the inequalities $0 \le n_v \le \#H_v$ must hold. Indeed, since π and its complex conjugate $\rho(\pi)$ are algebraic integers with product q, we have

$$0 \le v(\pi) = v(q) - v(\rho(\pi)) \le v(q),$$

whence follow the bounds on n_v.

Thus, the proof will be complete if we can show that there exists a CM field L containing π, such that

$$n_v := (\#H_v)\frac{v(\pi)}{v(q)}$$

is an integer for every valuation v of L dividing p.

Note that the denominators of

$$\frac{v(\pi)}{v(q)}$$

are bounded, even as L varies. Specifically, for any L containing π and any place v of L dividing p, there is a place w of $\mathbb{Q}[\pi]$ lying below v. But then we have

$$\frac{v(\pi)}{v(q)} = \frac{w\pi)}{w(q)}.$$

Since there are only finitely many places w of the field $\mathbb{Q}[\pi]$ lying over p, we can choose some positive integer D such that

$$D\frac{v(\pi)}{v(q)}$$

is an integer for all L and v.

Thus it is sufficient to choose some L such that, for every place v of L, the degree $\#H_v = (L_v : \mathbb{Q}_p)$ is divisible by D. This is easily achieved, for example by the following construction.

Let K_0 be the maximal totally real subfield of $\mathbb{Q}[\pi]$. (This is $\mathbb{Q}[\pi]$ itself if π is real, and $\mathbb{Q}[\pi + q/\pi]$ otherwise, as we have seen.) Let $\mathcal{O}_{k_0}$ denote its ring of integers. By weak approximation, we can choose a polynomial

$$p(x) = x^D + a_{D-1}x^{D-1} + \cdots + a_0 \in K_0[x]$$

such that (1) the coefficients a_i are in every prime ideal of $\mathcal{O}_{k_0}$ lying over p, (2) the coefficient a_0 is not in the square of any such prime ideal, and (3) for any embedding of K_0 in $\mathbb{C}$, the roots of p are all real. Then taking $L_0 = K_0[x]/p(x)$, we find (by a standard argument involving Newton polygons) that L_0 is a totally real field with all places above p ramified to a degree divisible by D. Taking $L = L_0[\pi]$ if π is not real, or $L = L_0[i]$ otherwise, completes the proof. □

Finally, we prove the result promised at the beginning of the section.

Corollary 5.5. *With notation as above, some power of π_A is equal to some power of π.*

Proof. Since q_A and q are both powers of p, we can choose positive integers M and N such that

$$q_A^M = q^N.$$

We claim that for any place v of L, we have

$$v(\pi_A^M) = v(\pi^N).$$

For v nonarchimedean and not dividing p, both sides are zero by the argument in Lemma 5.2. Similarly, at any archimedean place, both π_A^M and π^N have norm equal to $q_A^M = q^N$. Finally, at the places v dividing p, Theorem 5.4 guarantees that

$$\frac{v(\pi_A)}{v(q_A)} = \frac{v(\pi)}{v(q)},$$

from which the result follows.

Now let

$$\zeta = \frac{\pi_A^M}{\pi^N}.$$

We have $v(\zeta) = 0$ for every place ζ of L. Hence in particular ζ, and all its powers, are algebraic integers in the field L, all of whose archimedean norms are equal to 1. But there can be only finitely many such integers of a given degree; so some powers of ζ must be equal, whence ζ is a root of unity. Writing $\zeta^L = 1$, we have

$$\pi_A^{LM} = \pi^{LN},$$

as desired. □

6 Proof of Surjectivity

We now come (after a short definition) to the main theorem of these notes.

Definition 6.1. *A Weil p^a-number μ is said to be* effective *if it is in the image of the Honda-Tate map HT, that is, if there is a simple abelian variety defined over $\mathbb{F}_{p^a}$, the characteristic polynomial of whose Frobenius morphism has μ as a root. If we say that μ is effective without specifying p^a, we mean that there is some p^a for which μ is a Weil p^a-number, and μ is in the image of the corresponding Honda-Tate map.*

Theorem 6.2. *For every prime power q, every Weil q-number is effective.*

We have seen that, given π, there is some effective π_A such that some power of π_A is equal to some power of π. The following theorem will complete the proof.

Theorem 6.3. *Given μ a Weil p^a-number and N a positive integer, μ is effective if and only if μ^N is effective.*

Proof. One direction is trivial. Suppose μ is an effective Weil p^a-number, and let B be an abelian variety over F_{p^a} on which the relative Frobenius ϕ acts as μ. Then the base change of B to $\mathbb{F}_{p^{Na}}$ has Frobenius ϕ^N, so μ^N is effective as well.

For the other direction, suppose μ^N is effective for some simple abelian variety B over $\mathbb{F}_{p^{Na}}$. We need to construct an abelian variety over $\mathbb{F}_{p^a}$ on which the Frobenius acts as μ. We will do this via Weil restriction. Hence, we need to understand how the Frobenius action interacts with Weil restriction.

Lemma 6.4. *Let B be an abelian variety over a finite field $\mathbb{F}_{p^{Na}}$, and let $\operatorname{Res} B$ denote its Weil restriction to $\mathbb{F}_{p^a}$. If $f_B(t)$ and $f_{\operatorname{Res} B}(t)$ denote the characteristic polynomials of Frobenius acting on B and $\operatorname{Res} B$, respectively, then we have*

$$f_{\operatorname{Res} B}(t) = f_B(t^N).$$

A proof can be found in Section 9 of [Eis].

Returning to proof of Theorem 6.3, recall that we have μ^N effective for some simple abelian variety B over $\mathbb{F}_{p^{Na}}$. By Lemma 6.4, the Weil restriction $A' = \operatorname{Res} B$ is an abelian variety, not necessarily simple, over $\mathbb{F}_{p^a}$, such that μ is a root of the characteristic polynomial p of the Frobenius operator on A'. Decomposing A' as a direct sum of simple components, we see that μ must be a root of the characteristic polynomial of at least one such component. Thus, we find that μ is effective.

This completes the proof. □

References

[BLR] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron Models*, Springer-Verlag, Berlin, 1990.

[CCO] C-L. Chai, B. Conrad, and F. Oort, *Complex Multiplication and Lifting Problems*, American Mathematical Society, 2014.

[Eis] K. Eisenträger, *The Theorem of Honda and Tate.* http://math.stanford.edu/ conrad/vigregroup/vigre04/hondatate.pdf.

[Mu1] D. Mumford, *Abelian Varieties*, Hindustan Book Agency, New Delhi, 2012.